

## BACKGROUND OF THE INVENTION

### 1. Technical Field:

5  
The present invention relates in general to electronic communications and, in particular, to recording messaging sessions. Still more particularly, the present invention relates to encrypting a message entries of a messaging session and  
10 providing users with a common key for decrypting the messaging entries.

### 2. Description of the Related Art:

15 As the Internet and telephony expand, the ease of communications between individuals in different locations continues to expand as well. One type of electronic communication is supported by messaging which includes the use of computer systems and data communication equipment to convey  
20 messages from one person to another, as by e-mail, voice mail, unified communications, instant messaging, or fax.

25 While e-mail has already expanded into nearly every facet of the business world, other types of messaging continue to forge into use. For example, instant messaging systems are typically utilized in the context of an Internet-supported application that transfers text between multiple Internet users in real time.

In particular, the Internet Relay Chat (IRC) service is one

example of instant messaging that enables an Internet user to participate in an on-line conversation in real time with other users. An IRC channel, maintained by an IRC server, transmits the text typed by each user who has joined the channel to the other users who have joined the channel. An IRC client shows the names of the currently active channels, enables the user to join a channel, and then displays the other channel participant's words on individual lines so that the user can respond.

Similar to IRC, chat rooms are often available through on-line services and provide a data communication channel that links computers and permits users to converse by sending text messages to one another in real-time.

Instant messaging sessions continue to replace and/or supplement telephone conversations in business and personal contexts. For example, while a user is logged onto a web site, the user may converse with technical personnel or personal shoppers via an instant messaging session. In another example, employees may discuss a project utilizing an instant messaging session rather than a telephone conversation.

However, messaging systems, and in particular instant messaging systems, are limited in that confidential communications may be carried on, but no method of encrypting these confidential communications is made available.

In view of the foregoing, it would be advantageous to provide a method, system and program for recording and encrypting

messaging sessions such that only users with a decryption key have access to the recorded messaging session.

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34  
35  
36  
37  
38  
39  
40  
41  
42  
43  
44  
45  
46  
47  
48  
49  
50  
51  
52  
53  
54  
55  
56  
57  
58  
59  
60  
61  
62  
63  
64  
65  
66  
67  
68  
69  
70  
71  
72  
73  
74  
75  
76  
77  
78  
79  
80  
81  
82  
83  
84  
85  
86  
87  
88  
89  
90  
91  
92  
93  
94  
95  
96  
97  
98  
99  
100  
101  
102  
103  
104  
105  
106  
107  
108  
109  
110  
111  
112  
113  
114  
115  
116  
117  
118  
119  
120  
121  
122  
123  
124  
125  
126  
127  
128  
129  
130  
131  
132  
133  
134  
135  
136  
137  
138  
139  
140  
141  
142  
143  
144  
145  
146  
147  
148  
149  
150  
151  
152  
153  
154  
155  
156  
157  
158  
159  
160  
161  
162  
163  
164  
165  
166  
167  
168  
169  
170  
171  
172  
173  
174  
175  
176  
177  
178  
179  
180  
181  
182  
183  
184  
185  
186  
187  
188  
189  
190  
191  
192  
193  
194  
195  
196  
197  
198  
199  
200  
201  
202  
203  
204  
205  
206  
207  
208  
209  
210  
211  
212  
213  
214  
215  
216  
217  
218  
219  
220  
221  
222  
223  
224  
225  
226  
227  
228  
229  
230  
231  
232  
233  
234  
235  
236  
237  
238  
239  
240  
241  
242  
243  
244  
245  
246  
247  
248  
249  
250  
251  
252  
253  
254  
255  
256  
257  
258  
259  
260  
261  
262  
263  
264  
265  
266  
267  
268  
269  
270  
271  
272  
273  
274  
275  
276  
277  
278  
279  
280  
281  
282  
283  
284  
285  
286  
287  
288  
289  
290  
291  
292  
293  
294  
295  
296  
297  
298  
299  
300  
301  
302  
303  
304  
305  
306  
307  
308  
309  
310  
311  
312  
313  
314  
315  
316  
317  
318  
319  
320  
321  
322  
323  
324  
325  
326  
327  
328  
329  
330  
331  
332  
333  
334  
335  
336  
337  
338  
339  
340  
341  
342  
343  
344  
345  
346  
347  
348  
349  
350  
351  
352  
353  
354  
355  
356  
357  
358  
359  
360  
361  
362  
363  
364  
365  
366  
367  
368  
369  
370  
371  
372  
373  
374  
375  
376  
377  
378  
379  
380  
381  
382  
383  
384  
385  
386  
387  
388  
389  
390  
391  
392  
393  
394  
395  
396  
397  
398  
399  
400  
401  
402  
403  
404  
405  
406  
407  
408  
409  
410  
411  
412  
413  
414  
415  
416  
417  
418  
419  
420  
421  
422  
423  
424  
425  
426  
427  
428  
429  
430  
431  
432  
433  
434  
435  
436  
437  
438  
439  
440  
441  
442  
443  
444  
445  
446  
447  
448  
449  
450  
451  
452  
453  
454  
455  
456  
457  
458  
459  
460  
461  
462  
463  
464  
465  
466  
467  
468  
469  
470  
471  
472  
473  
474  
475  
476  
477  
478  
479  
480  
481  
482  
483  
484  
485  
486  
487  
488  
489  
490  
491  
492  
493  
494  
495  
496  
497  
498  
499  
500  
501  
502  
503  
504  
505  
506  
507  
508  
509  
510  
511  
512  
513  
514  
515  
516  
517  
518  
519  
520  
521  
522  
523  
524  
525  
526  
527  
528  
529  
530  
531  
532  
533  
534  
535  
536  
537  
538  
539  
540  
541  
542  
543  
544  
545  
546  
547  
548  
549  
550  
551  
552  
553  
554  
555  
556  
557  
558  
559  
560  
561  
562  
563  
564  
565  
566  
567  
568  
569  
570  
571  
572  
573  
574  
575  
576  
577  
578  
579  
580  
581  
582  
583  
584  
585  
586  
587  
588  
589  
590  
591  
592  
593  
594  
595  
596  
597  
598  
599  
600  
601  
602  
603  
604  
605  
606  
607  
608  
609  
610  
611  
612  
613  
614  
615  
616  
617  
618  
619  
620  
621  
622  
623  
624  
625  
626  
627  
628  
629  
630  
631  
632  
633  
634  
635  
636  
637  
638  
639  
640  
641  
642  
643  
644  
645  
646  
647  
648  
649  
650  
651  
652  
653  
654  
655  
656  
657  
658  
659  
660  
661  
662  
663  
664  
665  
666  
667  
668  
669  
670  
671  
672  
673  
674  
675  
676  
677  
678  
679  
680  
681  
682  
683  
684  
685  
686  
687  
688  
689  
690  
691  
692  
693  
694  
695  
696  
697  
698  
699  
700  
701  
702  
703  
704  
705  
706  
707  
708  
709  
710  
711  
712  
713  
714  
715  
716  
717  
718  
719  
720  
721  
722  
723  
724  
725  
726  
727  
728  
729  
730  
731  
732  
733  
734  
735  
736  
737  
738  
739  
740  
741  
742  
743  
744  
745  
746  
747  
748  
749  
750  
751  
752  
753  
754  
755  
756  
757  
758  
759  
760  
761  
762  
763  
764  
765  
766  
767  
768  
769  
770  
771  
772  
773  
774  
775  
776  
777  
778  
779  
780  
781  
782  
783  
784  
785  
786  
787  
788  
789  
790  
791  
792  
793  
794  
795  
796  
797  
798  
799  
800  
801  
802  
803  
804  
805  
806  
807  
808  
809  
810  
811  
812  
813  
814  
815  
816  
817  
818  
819  
820  
821  
822  
823  
824  
825  
826  
827  
828  
829  
830  
831  
832  
833  
834  
835  
836  
837  
838  
839  
840  
841  
842  
843  
844  
845  
846  
847  
848  
849  
850  
851  
852  
853  
854  
855  
856  
857  
858  
859  
860  
861  
862  
863  
864  
865  
866  
867  
868  
869  
870  
871  
872  
873  
874  
875  
876  
877  
878  
879  
880  
881  
882  
883  
884  
885  
886  
887  
888  
889  
890  
891  
892  
893  
894  
895  
896  
897  
898  
899  
900  
901  
902  
903  
904  
905  
906  
907  
908  
909  
910  
911  
912  
913  
914  
915  
916  
917  
918  
919  
920  
921  
922  
923  
924  
925  
926  
927  
928  
929  
930  
931  
932  
933  
934  
935  
936  
937  
938  
939  
940  
941  
942  
943  
944  
945  
946  
947  
948  
949  
950  
951  
952  
953  
954  
955  
956  
957  
958  
959  
960  
961  
962  
963  
964  
965  
966  
967  
968  
969  
970  
971  
972  
973  
974  
975  
976  
977  
978  
979  
980  
981  
982  
983  
984  
985  
986  
987  
988  
989  
990  
991  
992  
993  
994  
995  
996  
997  
998  
999  
1000  
1001  
1002  
1003  
1004  
1005  
1006  
1007  
1008  
1009  
1010  
1011  
1012  
1013  
1014  
1015  
1016  
1017  
1018  
1019  
1020  
1021  
1022  
1023  
1024  
1025  
1026  
1027  
1028  
1029  
1030  
1031  
1032  
1033  
1034  
1035  
1036  
1037  
1038  
1039  
1040  
1041  
1042  
1043  
1044  
1045  
1046  
1047  
1048  
1049  
1050  
1051  
1052  
1053  
1054  
1055  
1056  
1057  
1058  
1059  
1060  
1061  
1062  
1063  
1064  
1065  
1066  
1067  
1068  
1069  
1070  
1071  
1072  
1073  
1074  
1075  
1076  
1077  
1078  
1079  
1080  
1081  
1082  
1083  
1084  
1085  
1086  
1087  
1088  
1089  
1090  
1091  
1092  
1093  
1094  
1095  
1096  
1097  
1098  
1099  
1100  
1101  
1102  
1103  
1104  
1105  
1106  
1107  
1108  
1109  
1110  
1111  
1112  
1113  
1114  
1115  
1116  
1117  
1118  
1119  
1120  
1121  
1122  
1123  
1124  
1125  
1126  
1127  
1128  
1129  
1130  
1131  
1132  
1133  
1134  
1135  
1136  
1137  
1138  
1139  
1140  
1141  
1142  
1143  
1144  
1145  
1146  
1147  
1148  
1149  
1150  
1151  
1152  
1153  
1154  
1155  
1156  
1157  
1158  
1159  
1160  
1161  
1162  
1163  
1164  
1165  
1166  
1167  
1168  
1169  
1170  
1171  
1172  
1173  
1174  
1175  
1176  
1177  
1178  
1179  
1180  
1181  
1182  
1183  
1184  
1185  
1186  
1187  
1188  
1189  
1190  
1191  
1192  
1193  
1194  
1195  
1196  
1197  
1198  
1199  
1200  
1201  
1202  
1203  
1204  
1205  
1206  
1207  
1208  
1209  
1210  
1211  
1212  
1213  
1214  
1215  
1216  
1217  
1218  
1219  
1220  
1221  
1222  
1223  
1224  
1225  
1226  
1227  
1228  
1229  
1230  
1231  
1232  
1233  
1234  
1235  
1236  
1237  
1238  
1239  
1240  
1241  
1242  
1243  
1244  
1245  
1246  
1247  
1248  
1249  
1250  
1251  
1252  
1253  
1254  
1255  
1256  
1257  
1258  
1259  
1260  
1261  
1262  
1263  
1264  
1265  
1266  
1267  
1268  
1269  
1270  
1271  
1272  
1273  
1274  
1275  
1276  
1277  
1278  
1279  
1280  
1281  
1282  
1283  
1284  
1285  
1286  
1287  
1288  
1289  
1290  
1291  
1292  
1293  
1294  
1295  
1296  
1297  
1298  
1299  
1300  
1301  
1302  
1303  
1304  
1305  
1306  
1307  
1308  
1309  
1310  
1311  
1312  
1313  
1314  
1315  
1316  
1317  
1318  
1319  
1320  
1321  
1322  
1323  
1324  
1325  
1326  
1327  
1328  
1329  
1330  
1331  
1332  
1333  
1334  
1335  
1336  
1337  
1338  
1339  
1340  
1341  
1342  
1343  
1344  
1345  
1346  
1347  
1348  
1349  
1350  
1351  
1352  
1353  
1354  
1355  
1356  
1357  
1358  
1359  
1360  
1361  
1362  
1363  
1364  
1365  
1366  
1367  
1368  
1369  
1370  
1371  
1372  
1373  
1374  
1375  
1376  
1377  
1378  
1379  
1380  
1381  
1382  
1383  
1384  
1385  
1386  
1387  
1388  
1389  
1390  
1391  
1392  
1393  
1394  
1395  
1396  
1397  
1398  
1399  
1400  
1401  
1402  
1403  
1404  
1405  
1406  
1407  
1408  
1409  
1410  
1411  
1412  
1413  
1414  
1415  
1416  
1417  
1418  
1419  
1420  
1421  
1422  
1423  
1424  
1425  
1426  
1427  
1428  
1429  
1430  
1431  
1432  
1433  
1434  
1435  
1436  
1437  
1438  
1439  
1440  
1441  
1442  
1443  
1444  
1445  
1446  
1447  
1448  
1449  
1450  
1451  
1452  
1453  
1454  
1455  
1456  
1457  
1458  
1459  
1460  
1461  
1462  
1463  
1464  
1465  
1466  
1467  
1468  
1469  
1470  
1471  
1472  
1473  
1474  
1475  
1476  
1477  
1478  
1479  
1480  
1481  
1482  
1483  
1484  
1485  
1486  
1487  
1488  
1489  
1490  
1491  
1492  
1493  
1494  
1495  
1496  
1497  
1498  
1499  
1500  
1501  
1502  
1503  
1504  
1505  
1506  
1507  
1508  
1509  
1510  
1511  
1512  
1513  
1514  
1515  
1516  
1517  
1518  
1519  
1520  
1521  
1522  
1523  
1524  
1525  
1526  
1527  
1528  
1529  
1530  
1531  
1532  
1533  
1534  
1535  
1536  
1537  
1538  
1539  
1540  
1541  
1542  
1543  
1544  
1545  
1546  
1547  
1548  
1549  
1550  
1551  
1552  
1553  
1554  
1555  
1556  
1557  
1558  
1559  
1560  
1561  
1562  
1563  
1564  
1565  
1566  
1567  
1568  
1569  
1570  
1571  
1572  
1573  
1574  
1575  
1576  
1577  
1578  
1579  
1580  
1581  
1582  
1583  
1584  
1585  
1586  
1587  
1588  
1589  
1590  
1591  
1592  
1593  
1594  
1595  
1596  
1597  
1598  
1599  
1600  
1601  
1602  
1603  
1604  
1605  
1606  
1607  
1608  
1609  
1610  
1611  
1612  
1613  
1614  
1615  
1616  
1617  
1618  
1619  
1620  
1621  
1622  
1623  
1624  
1625  
1626  
1627  
1628  
1629  
1630  
1631  
1632  
1633  
1634  
1635  
1636  
1637  
1638  
1639  
1640  
1641  
1642  
1643  
1644  
1645  
1646  
1647  
1648  
1649  
1650  
1651  
1652  
1653  
1654  
1655  
1656  
1657  
1658  
1659  
1660  
1661  
1662  
1663  
1664  
1665  
1666  
1667  
1668  
1669  
1670  
1671  
1672  
1673  
1674  
1675  
1676  
1677  
1678  
1679  
1680  
1681  
1682  
1683  
1684  
1685  
1686  
1687  
1688  
1689  
1690  
1691  
1692  
1693  
1694  
1695  
1696  
1697  
1698  
1699  
1700  
1701  
1702  
1703  
1704  
1705  
1706  
1707  
1708  
1709  
1710  
1711  
1712  
1713  
1714  
1715  
1716  
1717  
1718  
1719  
1720  
1721  
1722  
1723  
1724  
1725  
1726  
1727  
1728  
1729  
1730  
1731  
1732  
1733  
1734  
1735  
1736  
1737  
1738  
1739  
1740  
1741  
1742  
1743  
1744  
1745  
1746  
1747  
1748  
1749  
1750  
1751  
1752  
1753  
1754  
1755  
1756  
1757  
1758  
1759  
1760  
1761  
1762  
1763  
1764  
1765  
1766  
1767  
1768  
1769  
1770  
1771  
1772  
1773  
1774  
1775  
1776  
1777  
1778  
1779  
1780  
1781  
1782  
1783  
1784  
1785  
1786  
1787  
1788  
1789  
1790  
1791  
1792  
1793  
1794  
1795  
1796  
1797  
1798  
1799  
1800  
1801  
1802  
1803  
1804  
1805  
1806  
1807  
1808  
1809  
1810  
1811  
1812  
1813  
1814  
1815  
1816  
1817  
1818  
1819  
1820  
1821  
1822  
1823  
1824  
1825  
1826  
1827  
1828  
1829  
1830  
1831  
1832  
1833  
1834  
1835  
1836  
1837  
1838  
1839  
1840  
1841  
1842  
1843  
1844  
1845  
1846  
1847  
1848  
1849  
1850  
1851  
1852  
1853  
1854  
1855  
1856  
1857  
1858  
1859  
1860  
1861  
1862  
1863  
1864  
1865  
1866  
1867  
1868  
1869  
1870  
1871  
1872  
1873  
1874  
1875  
1876  
1877  
1878  
1879  
1880  
1881  
1882  
1883  
1884  
1885  
1886  
1887  
1888  
1889  
1890  
1891  
1892  
1893  
1894  
1895  
1896  
1897  
1898  
1899  
1900  
1901  
1902  
1903  
1904  
1905  
1906  
1907  
1908  
1909  
1910  
1911  
1912  
1913  
1914  
1915  
1916  
1917  
1918  
1919  
1920  
1921  
1922  
1923  
1924  
1925  
1926  
1927  
1928  
1929  
1930  
1931  
1932  
1933  
1934  
1935  
1936  
1937  
1938  
1939  
1940  
1941  
1942  
1943  
1944  
1945  
1946  
1947  
1948  
1949  
1950  
1951  
1952  
1953  
1954  
1955  
1956  
1957  
1958  
1959  
1960  
1961  
1962  
1963  
1964  
1965  
1966  
1967  
1968  
1969  
1970  
1971  
1972  
1973  
1974  
1975  
1976  
1977  
1978  
1979  
1980  
1981  
1982  
1983  
1984  
1985  
1986  
1987  
1988  
1989  
1990  
1991  
1992  
1993  
1994  
1995  
1996  
1997  
1998  
1999  
2000  
2001  
2002  
2003  
2004  
2005  
2006  
2007  
2008  
2009  
2010  
2011  
2012  
2013  
2014  
2015  
2016  
2017  
2018  
2019  
2020  
2021  
2022  
2023  
2024  
2025  
2026  
2027  
2028  
2029  
2030  
2031  
2032  
2033  
2034  
2035  
2036  
2037  
2038  
2039  
2040  
2041  
2042  
2043  
2044  
2045  
2046  
2047  
2048  
2049  
2050  
2051  
2052  
2053  
2054  
2055  
2056  
2057  
2058  
2059  
2060  
2061  
2062  
2063  
2064  
2065  
2066  
2067  
2068  
2069  
2070  
2071  
2072  
2073  
2074  
2075  
2076  
2077  
2078  
2079  
2080  
2081  
2082  
2083  
2084  
2085  
2086  
2087  
2088  
2089  
2090  
2091  
2092  
2093  
2094  
2095  
2096  
2097  
2098  
2099  
2100  
2101  
2102  
2103  
2104  
2105  
2106  
2107  
2108  
2109  
2110  
2111  
2112  
2113  
2114  
2115  
2116  
2117  
2118  
2119  
2120  
2121  
2122  
2123  
2124  
2125  
2126  
2127  
2128  
2129  
2130  
2131  
2132  
2133  
2134  
2135  
2136  
2137  
2138  
2139  
2140  
2141  
2142  
2143  
2144  
2145  
2146  
2147  
2148  
2149  
2150  
2151  
2152  
2153  
2154  
2155  
2156  
2157  
2158  
2159  
2160  
2161  
2162  
2163  
2164  
2165  
2166  
2167  
2168  
2169  
2170  
2171  
2172  
2173  
2174  
2175  
2176  
2177  
2178  
2179  
2180  
2181  
2182  
2183  
2184  
2185  
2186  
2187  
2188  
2189  
2190  
2191  
2192  
2193  
2194  
2195  
2196  
2197  
2198  
2199  
2200  
2201  
2202  
2203  
2204  
2205  
2206  
2207  
2208  
2209  
2210  
2211  
2212  
2213  
2214  
2215  
2216  
2217  
2218  
2219  
2220  
2221  
2222  
2223  
2224

### SUMMARY OF THE INVENTION

In view of the foregoing, it is therefore an object of the present invention to provide an improved method, system and program for performing electronic communications.

It is another object of the present invention to provide a method, system and program for recording messaging sessions.

It is yet another object of the present invention to provide a method, system and program for encrypting a message entries within a messaging session and providing users with a key for decrypting the message entries.

According to one aspect of the present invention, a recording of a messaging session is encrypted with a symmetric key, wherein the symmetric key is enabled to decrypt the encrypted recording of the messaging session. The symmetric key is encoded with multiple public keys, each corresponding with one of multiple users, wherein the encoded symmetric key is decodable by each of the users, such that the encrypted recording of the messaging session is decryptable by each of the users utilizing the symmetric key.

According to another aspect of the present invention, a message entry is encrypted with a symmetric key at a client messaging system. The encrypted messaging entry is then transmitted for distribution to multiple recipient client

messaging systems, such that the message entry is encrypted with the symmetric key enabled to decrypt the message entry prior to transmission across a network.

5 All objects, features, and advantages of the present invention will become apparent in the following detailed written description.

10  
15  
20  
25  
30  
35  
40  
45  
50  
55  
60  
65  
70  
75  
80  
85  
90  
95  
100  
105  
110  
115  
120  
125  
130  
135  
140  
145  
150  
155  
160  
165  
170  
175  
180  
185  
190  
195  
200  
205  
210  
215  
220  
225  
230  
235  
240  
245  
250  
255  
260  
265  
270  
275  
280  
285  
290  
295  
300  
305  
310  
315  
320  
325  
330  
335  
340  
345  
350  
355  
360  
365  
370  
375  
380  
385  
390  
395  
400  
405  
410  
415  
420  
425  
430  
435  
440  
445  
450  
455  
460  
465  
470  
475  
480  
485  
490  
495  
500  
505  
510  
515  
520  
525  
530  
535  
540  
545  
550  
555  
560  
565  
570  
575  
580  
585  
590  
595  
600  
605  
610  
615  
620  
625  
630  
635  
640  
645  
650  
655  
660  
665  
670  
675  
680  
685  
690  
695  
700  
705  
710  
715  
720  
725  
730  
735  
740  
745  
750  
755  
760  
765  
770  
775  
780  
785  
790  
795  
800  
805  
810  
815  
820  
825  
830  
835  
840  
845  
850  
855  
860  
865  
870  
875  
880  
885  
890  
895  
900  
905  
910  
915  
920  
925  
930  
935  
940  
945  
950  
955  
960  
965  
970  
975  
980  
985  
990  
995

### BRIEF DESCRIPTION OF THE DRAWINGS

The novel features believed characteristic of the invention are set forth in the appended claims. The invention itself  
5 however, as well as a preferred mode of use, further objects and advantages thereof, will best be understood by reference to the following detailed description of an illustrative embodiment when read in conjunction with the accompanying drawings, wherein:

10 **Figure 1** depicts one embodiment of a computer system with which the method, system and program of the present invention may advantageously be utilized;

15 **Figure 2** illustrates a simplified block diagram of a client/server environment in which electronic messaging typically takes place in accordance with the method, system and program of the present invention;

20 **Figure 3** depicts a block diagram of one embodiment of a messaging server in accordance with the method, system and program of the present invention;

25 **Figure 4** illustrates a block diagram of one embodiment of a real-time encryption system in accordance with the method, system, and program of the present invention;

**Figure 5** depicts a graphical representation of a messaging session interface in accordance with the method, system and program of the present invention;

**Figure 6** illustrates a block diagram of an encoded symmetric key in accordance with the method system and program of the present invention;

5       **Figure 7** depicts a high level logic flowchart of a process and program for controlling encryption and recording of messaging sessions in accordance with the method, system, and program of the present invention; and

10       **Figure 8** illustrates a high level logic flowchart of a process and program for controlling a client messaging system in accordance with the method, system and program of the present invention.

### DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

A method, system and program are provided for generating a symmetric key, encrypting a recorded messaging session with the symmetric key, and distributing the encrypted recorded messaging session.

A "messaging session" preferably includes, but is not limited to, any combination of voice, graphical, video, and/or text messages, instant and/or delayed, transmitted between multiple users via a network. Message entries within a messaging session may further included embedded text, video, still pictures, audio and other communication media. Messaging sessions may include use of on-line meetings, chat rooms, instant messages, e-mail, IRC, conference calling and other network methods of providing a channel for users to communicate within. Further, messaging sessions may include communications such as voice, video, and text transmissions between multiple telephony devices.

A "symmetric key", or common key, is preferably an autoencryption key that may be generated utilizing multiple encryption methods. In a preferred embodiment, the public keys of users participating in a messaging session are utilized to encode the symmetric key before transmission to the users.

In the following description, for the purposes of explanation, numerous specific details are set forth in order to provide a thorough understanding of the present invention. It



will be apparent, however, to one skilled in the art that the present invention may be practiced without these specific details. In other instances, well-known structures and devices are shown in block diagram form in order to avoid unnecessarily obscuring the present invention.

#### HARDWARE OVERVIEW

The present invention may be executed in a variety of systems, including a variety of computing systems and electronic devices under a number of different operating systems. In one embodiment of the present invention, the messaging system is a portable computing system such as a notebook computer, a palmtop computer, a personal digital assistant, a telephone or other electronic computing system that may also incorporate communications features that provide for telephony, enhanced telephony, messaging and information services. However, the messaging system may also be, for example, a desktop computer, a network computer, a midrange computer, a server system or a mainframe computer. Therefore, in general, the present invention is preferably executed in a computer system that performs computing tasks such as manipulating data in storage that is accessible to the computer system. In addition, the computer system preferably includes at least one output device and at least one input device.

Referring now to the drawings and in particular to **Figure 1**, there is depicted one embodiment of a computer system with which the method, system and program of the present invention may

advantageously be utilized. Computer system 10 comprises a bus 22 or other communication device for communicating information within computer system 10, and at least one processing device such as processor 12, coupled to bus 22 for processing information. Bus 22 preferably includes low-latency and high-latency paths that are connected by bridges and controlled within computer system 10 by multiple bus controllers.

Processor 12 may be a general-purpose processor such as IBM's PowerPC™ processor that, during normal operation, processes data under the control of operating system and application software stored in a dynamic storage device such as random access memory (RAM) 14 and a static storage device such as Read Only Memory (ROM) 16. The operating system preferably provides a graphical user interface (GUI) to the user. In a preferred embodiment, application software contains machine executable instructions that when executed on processor 12 carry out the operations depicted in the flowcharts of FIG. 7, 8, and others described herein. Alternatively, the steps of the present invention might be performed by specific hardware components that contain hardwire logic for performing the steps, or by any combination of programmed computer components and custom hardware components.

The present invention may be provided as a computer program product, included on a machine-readable medium having stored thereon the machine executable instructions used to program computer system 10 to perform a process according to the present

invention. The term "machine-readable medium" as used herein includes any medium that participates in providing instructions to processor 12 or other components of computer system 10 for execution. Such a medium may take many forms including, but not limited to, non-volatile media, volatile media, and transmission media. Common forms of non-volatile media include, for example, a floppy disk, a flexible disk, a hard disk, magnetic tape or any other magnetic medium, a compact disc ROM (CD-ROM) or any other optical medium, punch cards or any other physical medium with patterns of holes, a programmable ROM (PROM), an erasable PROM (EPROM), electrically EPROM (EEPROM), a flash memory, any other memory chip or cartridge, or any other medium from which computer system 10 can read and which is suitable for storing instructions. In the present embodiment, an example of non-volatile media is storage device 18. Volatile media includes dynamic memory such as RAM 14. Transmission media includes coaxial cables, copper wire or fiber optics, including the wires that comprise bus 22. Transmission media can also take the form of acoustic or light waves, such as those generated during radio wave or infrared data communications.

Moreover, the present invention may be downloaded as a computer program product, wherein the program instructions may be transferred from a remote computer such as a server 39 to requesting computer system 10 by way of data signals embodied in a carrier wave or other propagation medium via a network link 34 (e.g., a modem or network connection) to a communications interface 32 coupled to bus 22. Communications interface 32

provides a two-way data communications coupling to network link 34 that may be connected, for example, to a local area network (LAN), wide area network (WAN), or as depicted herein, directly to an Internet Service Provider (ISP) 37. In particular, network link 34 may provide wired and/or wireless network communications to one or more networks.

ISP 37 in turn provides data communication services through the Internet 38 or other network. Internet 38 may refer to the worldwide collection of networks and gateways that use a particular protocol, such as Transmission Control Protocol (TCP) and Internet Protocol (IP), to communicate with one another. ISP 37 and Internet 38 both use electrical, electromagnetic, or optical signals that carry digital data streams. The signals through the various networks and the signals on network link 34 and through communication interface 32, which carry the digital data to and from computer system 10, are exemplary forms of carrier waves transporting the information.

Further, multiple peripheral components may be added to computer system 10. For example, an audio output 28 is attached to bus 22 for controlling audio output through a speaker or other audio projection device. A display 24 is also attached to bus 22 for providing visual, tactile or other graphical representation formats. A keyboard 26 and cursor control device 30, such as a mouse, trackball, or cursor direction keys, are coupled to bus 22 as interfaces for user inputs to computer system 10. In alternate embodiments of the present invention, additional input

and output peripheral components may be added.

#### MESSAGING SYSTEMS CONTEXT

5       With reference now to **Figure 2**, there is depicted a simplified block diagram of a client/server environment in which electronic messaging typically takes place in accordance with the method, system and program of the present invention. The client/server environment is implemented within multiple network  
10 architectures. For example, the architecture of the World Wide Web (the Web) follows a traditional client/server modeled environment.

15       The terms "client" and "server" are used to refer to a computer's general role as a requester of data (the client) or provider of data (the server). In the Web environment, web browsers such as Netscape Navigator typically reside on client messaging systems **40a-40n** and render Web documents (pages) served by at least one messaging server such as messaging server **42**.  
20 Additionally, each of client messaging systems **40a-40n** and messaging server **42** may function as both a "client" and a "server" and may be implemented utilizing a computer system such as computer system **10** of **Figure 1**. Further, while the present invention is described with emphasis upon messaging server **42**  
25 controlling a messaging session, the present invention may also be performed by client messaging systems **40a-40n** engaged in peer-to-peer network communications via a network **44**.

The Web may refer to the total set of interlinked hypertext documents residing on servers all around the world. Network **44**, such as the Internet, provides an infrastructure for transmitting these hypertext documents between client messaging systems **40a-40n** and messaging server **42**. Documents (pages) on the Web may be written in multiple languages, such as Hypertext Markup Language (HTML) or Extensible Markup Language (XML), and identified by Uniform Resource Indicators (URIs) that specify the particular messaging server **42** and pathname by which a file can be accessed, and then transmitted from messaging server **42** to an end user utilizing a protocol such as Hypertext Transfer Protocol (HTTP). Web pages may further include text, graphic images, movie files, and sounds as well as Java applets and other small embedded software programs that execute when the user activates them by clicking on a link.

Advantageously, in the present invention, a client enters a message via one of messaging input/output (I/O) devices **46a-46n** for a messaging session at a client messaging system such as client messaging system **40a**. The message entry is transmitted to messaging server **42**. Messaging server **42** then distributes the message entry to the user participating in the messaging session via network **44**.

In addition, in the present invention, a user at each of client messaging systems **40a-40n** may request to record or log a messaging session. Such requests are transmitted to messaging server **42**. Messaging server **42** may then record the messaging

session until the user at one of client messaging systems **40a-40n** requests to stop logging. Then, the user at one of client messaging systems **40a-40n** may request that the recording be stored either as public text or as private text, which requires encoding.

If the recording is stored as public text at messaging server **42**, client messaging systems **40a-40n**, or another data storage system accessible via network **44**, then any user may access the recording. Public text, as well as private text, may include alternate security devices and verification devices such as watermarking and digital signatures attached thereto.

However, if the recording is stored as private text, then first a symmetric key is generated by messaging server **42**. The symmetric key is utilized by messaging server **42** to encrypt the recording of the messaging session. Then, the symmetric key is encoded with the public keys of each user participating in the messaging session, such that the symmetric key is secure from tampering and can be utilized for easy encryption and decryption. The encrypted messaging session is then stored at messaging server **42**, client messaging systems **40a-40n**, or other data storage systems accessible via network **44**. Advantageously, the symmetric key may be stored at a secure location, such that the symmetric key may be recovered if it is lost.

In particular, a user may be given the option to record text as private text, in which case encryption is automatically

performed. Alternatively, a user may be given the option to select to generate the symmetric key, request that the symmetric key be encoded and transmitted to a selection of users and then request that the recorded messaging session be encrypted and transmitted to the selection of users. In addition, a user may select from alternate methods of encryption or alternate levels of encryption.

While in the present embodiment messaging server **42** handles transmission of message entries, recording of messaging sessions and encryption thereof, in alternate embodiments, encrypted messaging sessions and encoded symmetric keys may be accessible to client messaging systems **40a-40n** as files in a directory that is accessible to a user. In addition, the encrypted messaging sessions and encoded symmetric keys may be transmitted as e-mail to participants in the messaging session, where the e-mail application functioning on the client messaging system automatically determines that the e-mail contains an encrypted messaging session and decodes the symmetric key and then decrypts the encrypted messaging session with the decoded symmetric key. Moreover, the present invention may utilize a traditional IRC channel for transmitting message entries and a special IRC device channel opened in parallel with the traditional IRC channel for transmitting the encoded symmetric keys and encrypted messaging sessions among users. Furthermore, other types of messaging systems may be utilized to implement the present invention, as will be understood by one skilled in the art.

Advantageously, the steps of requesting to record,



requesting to stop recording, and requesting that recordings be stored as public text or private text are performed by an application executing in each of client messaging systems **40a-40n**, such as client recording applications **41a-41n**. In addition, client recording applications **41a-41n** may control transmission of a public key for the user to messaging server **42**, and may perform steps of creating a symmetric key and encryption, particularly where client messaging systems **40a-40n** are communicating in a peer-to-peer network.

Referring now to **Figure 3**, there is illustrated a block diagram of one embodiment of a messaging server in accordance with the method, system and program of the present invention. As depicted messaging server **42** includes an encryption controller **62** that is provided to control the process steps of messaging server **42** as will be further described.

Messaging server **42** also includes multiple channels **52a-52n**. Each of channels **52a-52n** may represent a separate information path within messaging server **42** in which multiple users may participate in a messaging session. Messaging server **42** may have a defined number of channels **52a-52n** or may allow users to create new channels as needed. In particular, channels provide network paths between multiple users for both voice and text communications. Each of channels **52a-52n** may further include multiple distinguishable topics.

In addition, each of channels **52a-52n** preferably includes a

table of current users **54a-54n**. As a user selects to participate in channels **52a-52n**, the user's identification is attached to the table of current users **54a-54n** for that channel.

5 Preferably, as messaging server **42** receives messages, they may be stored according to the channel, topic and user and then distributed to each of the users participating in that channel. Where both voice and text are being utilized in a single messaging session, messaging server **42** may transmit both voice  
10 and text or messaging server **42** may translate all entries into either voice or text before distributing entries to the users participating in the channel.

15 Messaging entries are preferably stored within each channel in one of log files **51a-51n**. Advantageously, multiple users may request to record different selections of the message entries for a messaging session where a new log file is utilized for each request. For example, one user may request to record message entries from a selection of users from among all the users while  
20 another user may request to record message entries during a particular time interval of the messaging session.

25 When a user has finished recording the desired portions of a messaging session, the log file for that user may be stored in a log file repository **61**. In particular, in the present invention a user may select to store the log file as public text or private text. When a log file is stored as public text, no encryption is necessary for storing the log file in log file repository **61**.

However, when a log file is stored as private text, then the log file is encrypted according to the present invention prior to storage in log file repository **61**.

5        Advantageously, log file repository **61** catalogs messaging session recordings such that multiple users may easily access the recordings. While in the present invention log file repository **61** is depicted within messaging server **42**, in alternate embodiments log file repository **61** may be included in an  
10        alternate server system. Alternatively, log files may be transmitted from messaging server **42** to client messaging systems for storage or may be logged in one of the client messaging systems during the messaging session.

15        Messaging server **42** includes a user profiles database **60** that includes profile information for each user, including, but not limited to, a user identification, a name, an e-mail address, public key and a user history recorded as the user participates in messaging sessions. The user identification stored in user  
20        profiles **60** during registration is utilized across multiple channels for identifying entries provided by that user. The public key may be utilized to encode a symmetric key or other decryption key transmitted to a user. The user may then utilize a private key to decode the symmetric key and then utilize the  
25        symmetric key to decode the contents of a recorded messaging session.

Channel options are included with each channel as depicted

by channel options **58a-58n**. Channel options preferably include encryption levels required to record message entries within a messaging session. Advantageously, channel options may be selected when a user requests a new channel. Alternatively, a user may select a channel based on the encryption levels set in the channel options for that channel. Moreover, a business or other network service provider may automatically set channel options for each of channels **52a-52n**.

Encryption controller **62** is advantageously a software application executing within messaging server **42** to control the process of creating a symmetric key, encrypting a recorded messaging session with the symmetric key, encoding the symmetric key with user public keys and transmitting the encrypted messaging session to users.

A key repository **64** advantageously provides a storage device for storing symmetric keys generated to encrypt messaging sessions. In particular, a list of users sent each symmetric key may be stored such that the users included in the list may request the symmetric key when needed. In addition, the symmetric key is stored such that a system administrator, business, or other individual responsible for messaging server **42** is able to decrypt any recording encrypted by messaging server **42**.

With reference now to **Figure 4**, there is depicted a block diagram of one embodiment of a real-time encryption system in

accordance with the method, system, and program of the present invention. As illustrated, a messaging server **180** includes a database of current user public keys **182** and an encryption controller **184** in addition to other elements not illustrated.

5 Advantageously, when a user logs onto messaging server **180** from one of client messaging systems **190a-190n**, the public key for that user is transmitted to messaging server **180** for storage while the user is logged on. In addition, the public key for the user may be stored at an alternate location and retrieved into

10 the database of current user public keys **182** when the user is detected as having logged on.

According to one aspect of the present invention, encryption controller **184** may generate a symmetric key for encryption of a message entry and encode the symmetric key with the public key of

15 a user logged onto messaging server **180**. The encoded symmetric key is then transmitted to a client messaging system, such as client messaging system **190a**. A real-time crypton controller **192a** decodes the encoded symmetric key and encrypts the message entry with the symmetric key prior to transmittal to messaging

20 server **180**.

Messaging server **180** receives the encrypted message entry and encodes the symmetric key with the public keys of the

25 intended recipients of the encrypted message entry. Then, messaging server **180** distributes the encrypted message entry and encoded symmetric keys to multiple recipient client messaging systems, such as client messaging systems **190f** and **190n**. Real-

time crypton controllers **192f** and **192n** decode the symmetric key utilizing the matching private key and then decrypt the encrypted message entry with the symmetric key.

5        Alternatively, client messaging system **190a** may generate the symmetric key and encode the symmetric key with the public keys of intended recipients. Client messaging system **190a** will then distribute the encoded symmetric keys and encrypted message entry to client messaging systems **190f** and **190n**.

10        According to one advantage of the present invention, message entries are encrypted in real-time such that security of message entries is added during a messaging session, rather than just after the message entries are recorded. Further, an advantage of  
15        the present invention is that message entries are encrypted in real-time with a symmetric key such that multiple client messaging systems may receive and decrypt the encrypted message entry in real-time.

20        Referring now to **Figure 5**, there is depicted a graphical representation of a messaging session interface in accordance with the method, system and program of the present invention. As depicted, a messaging session interface **70** includes a messaging session window **72**. For the present example, messaging session  
25        interface **70** is accessible to user B, however in alternate embodiments, alternate users may have access to messaging session interface **70**.

Messaging session entries **74** are depicted within messaging session window **72**. Messaging session entries **74** include message entries by users A, B, and C and textual references to logging activity by user C. As illustrated within messaging session entries **74**, after user C requested to start logging, the message entries following are textually distinguishable in bold to indicate that the message entries are being recorded. Moreover, alternative types of indicators that message entries are being recorded may be utilized. For example, a graphical or audible indicator may be provided. In addition, as depicted within messaging session entries **74**, when user C requested to stop logging, user C then requested to encode and store the logging as private text.

Advantageously, messaging session window **72** may represent an on-line meeting where it is important to record and encrypt recordings of confidential information shared during the on-line meeting. Although one graphical example of a messaging session is depicted in the present invention, alternate types of graphical, video, audio, and textual messaging sessions may be utilized with the present invention.

A response block **76** is also illustrated within messaging session window **72**. Response block **76** is provided to allow a user to enter either a textual, graphical, or audible message to be included in the messaging session.

Messaging session interface **70** also includes multiple

selectable buttons **80**, **81**, **82** and **84**. In response to a user selecting selectable button **80**, a request to log the conversation is transmitted to the messaging server. In addition, in response to a user selecting selectable button **81**, a request to stop logging the conversation is transmitted to the messaging server.

In response to a user selecting selectable button **82**, a request is transmitted to the messaging server to store the portions of the messaging session logged by the user as public text. In storing the recorded messaging session as public text, the log file may be stored at client messaging systems, the messaging server or other data storage locations.

In response to a user selecting selectable button **84**, a request is transmitted to the messaging server that the portions of the messaging session logged by the user are encoded and stored as private text. Alternatively, where the client messaging systems are engaged in peer-to-peer communication, a user selection of selectable button **84** will cause the client messaging system to encode and store the recording.

In addition, in response to a user selection of selectable button **84** the user may be provided encryption options such as those depicted in graphical window **90**. For example, the user may select where to save the encrypted log file, including a log file repository and particular users, as illustrated at indicator **92**. In another example, the user may select a type of encryption to utilize, such as symmetric key encryption, as depicted at



indicator 94.

With reference now to **Figure 6**, there is a block diagram of an encoded symmetric key in accordance with the method system and program of the present invention. As illustrated, a symmetric key 92 has been generated as an encryption and decryption key for a recorded messaging session. In order to transmit the symmetric key to multiple users such that those users may decrypt the recorded messaging session, the symmetric key is encoded with a public key associated with each user as illustrated by reference numerals 94a-94n. The encoded symmetric keys are then transmitted according to the public key of the associated user.

One advantage of the present invention is that a single symmetric key is utilized for encryption and decryption such that even if user public keys change, the symmetric key may be utilized to decrypt the encrypted messaging session. In addition, the symmetric key can be stored at a secure site such that if a user loses the encoded symmetric key or the user changes public keys, then that user may access the symmetric key from the secure site.

Referring now to **Figure 7**, there is illustrated a high level logic flowchart of a process and program for controlling encryption and recording of messaging sessions in accordance with the method, system, and program of the present invention. As depicted, the process starts at block 100 and thereafter proceeds to block 102. Block 102 illustrates a determination as to which

event occurred when an event occurs. If a request to store a log file as public text is received, then the process passes to block 104. If a request to encode and store a log file as private text is received, then the process passes to block 120.

5

Block 104 depicts comparing the recorded message entries with public text criteria in the channel options and user preferences. In particular, channel options may designate particular keywords, topics, types of graphics, and other specified categories of message entries that may not be recorded as public text. In addition, user preferences for users participating in the messaging session may include specifications for categories of message entries that may not be recorded as public text.

10

15

Next, block 106 illustrates a determination as to whether or not the message entries meet the public text criteria. If the message entries meet the public text criteria, then the process passes to block 108. If the message entries do not meet the public text criteria, then the process passes to block 116.

20

Block 116 depicts transmitting a verification error indicating that the message entries may not be stored as public text; and the process ends.

25

Block 108 depicts transmitting a message verification indicating the message entries may be stored as public text. Next, block 110 illustrates saving the log file of recorded messaging entries into a log file repository. Thereafter, block

112 depicts a determination as to whether or not a local save is requested. In particular, a local save includes a request to transmit the log file to the requesting user and to other users participating in the messaging session. If a local save is not requested, then the process ends. If a local save is requested, then the process passes to block 114. Block 114 illustrates transmitting the log file to a designated selection of users and the process ends.

Block 120 illustrates generating a symmetric key. A symmetric key may include a combination of alphanumeric, graphics and audio. Next, block 122 depicts verifying the public keys of a designated selection of the users. Users may provide a public key in association with a user identification. In addition, even where a public key is stored in association with a user identification, users may be requested to verify that the public key is current. Thereafter, block 124 illustrates encoding the symmetric key according to the public keys and the process passes to block 126. In particular, when the symmetric key is encoded with a public key, each user is required to use a private key to decode the symmetric key, thereby protecting the symmetric key from tampering or from use by an unauthorized user.

Block 126 depicts transmitting the encoded symmetric keys according to public key to the associated user. Next, block 128 illustrates transmitting the symmetric key to a trusted server. Thereafter, block 130 depicts encoding the log file with the symmetric key. Further, block 132 illustrates storing the

encrypted log file in a log file repository and the process passes to block **134**.

Block **134** illustrates a determination as to whether or not a local save is requested. If a local save is not requested, then the process ends. If a local save is requested, then the process passes to block **136**. Block **136** depicts transmitting the encrypted log file to a designated selection of users and the process ends.

With reference now to **Figure 8**, there is illustrated a high level logic flowchart of a process and program for controlling a client messaging system in accordance with the method, system and program of the present invention. As depicted, the process starts at block **150** and thereafter proceeds to block **152**. Block **152** illustrates a determination as to which event occurred when an event occurs. If a selection to store public text is received, then the process passes to block **154**. If a selection to encode and store private text is received, then the process passes to block **170**. Or, if a request to open an encrypted log file is received, then the process passes to block **180**.

Block **154** depicts transmitting a request to store a recorded log file as public text. Next, block **156** illustrates a determination as to whether the storage is verified. If storage is verified, then the process passes to block **158** where a notification is output that the log file is stored as public text; and the process ends. If storage is not verified, then the

process passes to block **160** where a notification is output that the log file was not stored as public text; and the process ends.

Block **170** illustrates transmitting a request to encode and store a recorded log file as private text. Next, block **172** depicts a determination as to whether or not an encoded symmetric key and encrypted log file are received. If an encoded symmetric key and encrypted log file are not received, then the process ends. If an encoded symmetric key and encrypted log file are received, then the process passes to block **174**. Block **174** illustrates storing the encoded symmetric key and encrypted log file and the process ends.

Block **180** depicts decoding the encoded symmetric key with a private key. Next, block **182** illustrates decrypting the encrypted log file with the symmetric key and the process ends.

While the invention has been particularly shown and described with reference to a preferred embodiment, it will be understood by those skilled in the art that various changes in form and detail may be made therein without departing from the spirit and scope of the invention.